

Application No.: 09/928,491
Old Attorney's Docket No. 027557-061
New Attorney's Docket No. 0119-078
Page 2

Amendments to the Claims:

Please replace all prior versions, and listings of claims in the application with the following listing of claims.

Listing of claims

Claims 1-27 (cancelled)

Claim 28 (new): A method of operating a mobile communications device that includes a cryptographic module, the method comprising:

detecting whether a node accessed by the mobile communications device via a wireless network requires performance of an authentication, and in response to detecting that the node accessed by the mobile communications device via the wireless network requires performance of the authentication, using the cryptographic module to carry out the authentication; and

detecting whether a local external device having a connection to a network by means other than the mobile communications device requires performance of an authentication, and in response to detecting that the local external device requires performance of the authentication, using the cryptographic module to carry out the authentication.

Claim 29 (new): The method of claim 28, wherein the mobile communications device is a Wireless Application Protocol (WAP)-enabled device.

Claim 30 (new): The method of claim 29, wherein the cryptographic module is implemented in a Wireless Identity Module (WIM).

Claim 31 (new): The method of claim 29, wherein each of the authentications is carried out in accordance with Wireless Public Key Infrastructure.

Claim 32 (new): The method of claim 28, wherein communications between the mobile communications device and the local external device take place via a wired connection.

Application No.: 09/928,491
Old Attorney's Docket No. 027557-061
New Attorney's Docket No. 0119-078
Page 3

Claim 33 (new): The method of claim 28, wherein communications between the mobile communications device and the local external device take place via a wireless connection.

Claim 34 (new): A mobile communications device comprising:
a cryptographic module;
means for detecting whether a node accessed by the mobile communications device via a wireless network requires performance of an authentication, and in response to detecting that the node accessed by the mobile communications device via the wireless network requires performance of the authentication, uses the cryptographic module to carry out the authentication; and
means for detecting whether a local external device having a connection to a network by means other than the mobile communications device requires performance of an authentication, and in response to detecting that the local external device requires performance of the authentication, uses the cryptographic module to carry out the authentication.

Claim 35 (new): The mobile communications device of claim 34, wherein the mobile communications device is a Wireless Application Protocol (WAP)-enabled device.

Claim 36 (new): The mobile communications device of claim 35, wherein the cryptographic module is implemented in a Wireless Identity Module (WIM).

Claim 37 (new): The mobile communications device of claim 35, wherein each of the authentications is carried out in accordance with Wireless Public Key Infrastructure.

Claim 38 (new): The mobile communications device of claim 34, comprising:
means for communicating with the local external device via a wired connection.

Claim 39 (new): The mobile communications device of claim 34, comprising:
means for communicating with the local external device via a wireless connection.